Investigations into the Existence and Centralization of Equilibria in Bitcoin-like Auctions

Spring 2018

Primary Reader: Prof. Matt Weinberg
Second Reader: Prof. Jon Fickenscher

Dylan Mavrides

0 Introduction

In 2008, an individual or organization operating under the pseudonym Satoshi Nakamoto published a paper describing Bitcoin, a form of decentralized electronic currency. In the years since, Bitcoin has grown in popularity; today 1 Bitcoin trades for approximately 9150.68 USD [1]. One of the original goals of Bitcoin was for it to be decentralized - avoiding control of the currency by a single or few individuals or organizations. However, in practice, Bitcoin mining has become a relatively centralized process. Mining "pools" have been established, wherein a large number of individuals pool their computational power, and split any rewards proportionally.[1] Three mining pools account for over 50% of total mining, and thus, to some extent, it seems like Bitcoin has become centralized, even if not by design [2].

This investigation is a continuation of Weinberg's paper *Bitcoin: A Natural Oligopoly*, submission 283 to ACM Economics Computation 2018 (EC '18). His paper investigated the nature of equilibria in Bitcoin-like settings, concluding that small cost asymmetries and other changes result in Nash Equilibria where at most only a small number of agents choose to invest. The specific conclusions will be outlined below.

1 Initial Models and Summary of Prior Results

In the Bitcoin protocol itself, (potential) miners essentially choose to use some amount of computational power in the hope that they are the ones to first brute force the solution to a hash-function related "puzzle." [2] Thus we begin by introducing the most basic *proportional* model, in which n miners compete for a total prize of fixed size 1. We say that each miner i chooses to invest q_i, paying cost $c_i q_i$, receiving reward $x_i(q) = \frac{q_i}{\sum_j q_j}$, where $q = \langle q_i, ..., q_n \rangle$, giving utility $U_i(q) = x_i(q) - c_i q_i$. For purposes of simplicity, we assume that $c_1 \leq c_2 \leq ... \leq c_n$. We see that this model resembles an all-pay auction, except where the prize is divided proportionally according to investment.

Of course, in practice, reward may not be exactly proportional to one's investment. For instance, the cost of additional computational power may not scale linearly, or one may be able to take advantage of some small exploits in the Bitcoin protocol itself, if they acquire a large proportion of computational power relative to other miners. With this motivation, Weinberg addresses a model he calls *Economies of Scale*, in which everything is the same, except each miner instead receives reward $x_i(q) = \frac{q_i^\alpha}{\sum_j q_j^\alpha}$, where $\alpha > 1$.

The term "centralization" as used in this paper will refer to the number of miners who invest in equilibrium. We will consider a setting of miners with a set of costs, and then vary the reward function, and consider how centralization of the equilibrium for this set of miners changes. In particular, we will derive lower bounds on the proportion of investment miners will have as a function of the miners' costs. While Weinberg's paper gives initial bounds on centralization, we will show that with a class of changes to the reward function, we derive stronger bounds. We also note, however, that centralization is not tied to this definition. In particular, what we intuitively wish to capture is both the number of miners who choose to invest as well as the relative proportions of those who invest. It may also be appropriate to define centralization in terms of the variance in the proportions of investments made by the miners, or some other measure. For the purposes of this paper, we will call bounds for a new reward function *more centralized* if, given a set of costs, they give a lower upper bound on the number of people who will invest in equilibrium, when compared to an old reward function.

[1] This is because in practice, Bitcoins are a discrete quantity and rewarded with probability proportional to computational power, thus in joining a mining pool, one may sacrifice some expected value for lower variance in reward.

[2] Essentially they must brute force over random integers in the hope that they manage to hash an input based on this number and some transaction history to a specific value.

We briefly recall that a *Nash Equilibrium* (or simply "equilibrium") in this setting occurs when each miner invests an amount such that, if any miner were to unilaterally vary their investment, it would weakly-negatively impact their utility function. Thus in equilibrium, we have a state such that, if there are no external influences, no miner will act and thus the state is fixed.

With this in mind, Weinberg's results are quoted below,[3] up to minor reformatting:

Theorem 1.1: [3, 3.3] *In the proportional model, there exists a unique pure strategy nash equilibrium, q. It is defined as follows:*

Let $T_i = \sum_{j \leq i} c_j/(i-1)$ *then:*

(1) *Let* $i^* = \max\{i | c_i < T_i\}$

(2) *If* $i > i^*$, *then* $q_i = x_i = 0$.

(3) *If* $i \leq i^*$, *then* $q_i = \frac{1-c_i/T_i}{T_{i^*}}$, *and* $x_i(q) = 1 - c_i/T_{i^*}$.

Corollary 1.1.1: [3, 3.4] *In the proportional model, if miners have identical costs, then they all participate and invest*

$$\frac{n-1}{n^2 c_i}.$$

This corollary formalizes the way in which, in the simplest symmetrical case, we get decentralization, as here the variance of the proportion of investment among miners is 0, since they all have $1/n$ of the total investment.

Corollary 1.1.2: [3, 3.5] *In the proportional model, if miner i participates at all in the unique equilibrium, then* $x_j(q) \geq 1 - \frac{c_j}{c_i}$ for all j.
This shows that even with small cost asymmetries, we immediately get a significantly more centralized equilibrium. For instance, if miner i has costs 15% lower than another miner that participates in the equilibrium, then i must invest at least 15% of the total investment in the equilibrium. This gives strong constraints on the number of miners who can invest in equilibrium, given a set of costs, since the total percent of investment must not exceed 100.

Corollary 1.1.3: [3, 3.9] *In any equilibrium of the proportional model,* $c_i \geq c_j \implies q_j \geq q_i$.
In other words, a miner with lower cost must invest at least as much as a miner with higher cost.

Theorem 1.2: [3, 4.1] *Let q be any equilibrium in the EoS model. Then for all i,j (including i = j) such that* $q_i, q_j > 0$,

$$x_i(q) \geq 1 - \frac{1}{\alpha}\frac{c_i}{c_j}.$$

This theorem essentially extends Corollary 1.1.2 to the EoS model. We see that since now there is an extra $1/\alpha$ factor, and since $\alpha > 1$, this gives an even tighter constraint on decentralization, since the proportion of total investment that i must have, given costs c_i, c_j, is now greater. Taking $i = j$, we also get the following corollary:

Corollary 1.2.1: [3, 4.3] *Anyone who participates at all in the equilibrium must have market share at least* $1 - 1/\alpha$, *and thus the maximal number of participating miners is* $1 + \frac{1}{\alpha - 1}$.

Corollary 1.2.2: [3, 4.4] *Let q be any equilibrium of the EoS model, and let* $q_i \geq q_j > 0$, *then* $c_i \leq c_j$, *and equality holds if and only if* $q_i = q_j$.
We see that this corollary is similar to Corollary 1.1.3 in the proportional model.

[3]Note: the second value in the citation gives the theorem number in the original text.

Example 1: [3, A.4] *Let $c_i = 1 - 2^{-i-k}$ for any $k > 0$, then there is no equilibrium where finitely many miners participate, and although there exists an equilibrium for every prefix of $n < \infty$ miners, and the investment of miner i in these equilibria converges, there is no equilibrium in which finitely nor countably infinitely many miners participate.*
This is given as an example in the appendix of the original paper. The equilibria for each prefix follows from results given in the paper, and he proves the non-existence of equilibria in the infinite case as a proposition in the appendix as well.

2 Updated Models and Summary of My Results

The first route of investigation of this paper is to extend Weinberg's results to other reward models. As motivation, we consider an updated reward model we will refer to as the "popularity" factor model.

Example: The "Popularity" Factor Model

The following reward function intends to capture the idea that, as total investment increases, the value of the game's prize to the participants may increase. For instance, as a particular cryptocurrency gains popularity and more people invest in it, its exchange rate will likely increase, and thus the value of the currency itself may increase, even if the in-game reward is still fixed. We mimic this effect as follows:

For $0 \leq \beta < 1$:

$$y_i(q) = \frac{q_i^\alpha (\sum_j q_j)^\beta}{\sum_j q_j^\alpha}$$

Note that when $\beta = 0$, we reduce to the EoS case.

Generalized Multiplicative Factors

After some investigation into proving results similar to Weinberg's for several different multiplicative factors, a set of sufficient conditions for the multiplicative factor became clear. Thus we consider the more general case, where we scale the EoS reward function by some function $f(q_1, ..., q_n) \in \mathcal{F}$ where $\mathcal{F}$ is the family of positive, weakly-monotone-increasing functions that are symmetric with respect to their arguments. This makes sense, since the rewards can't have negative value, and no miner is in a distinguished position with respect to the game. We assume weakly-monotone-increasing due to an inequality we apply later in the proof, however, we may in fact make a slightly weaker assumption, as noted later.

Equilibria Considering Countably Infinitely Many Miners

As stated above, Weinberg's paper gives a sequence of costs such that, when considering the miners in cost-increasing order, there is an equilibrium when considering only any finite prefix of the miners, and the miners' costs converge, but there is no equilibrium when considering all of the miners. Here, under some basic assumptions, we provide necessary/sufficient conditions for which there exist equilibria in the countably infinitely many miners case.

Subgame Perfect Nash Equilibria in the Proportional Model

We also consider a different investment model, where each miner i has an opportunity to invest such that they invest in some sequence, where each miner sees how much the previous miners have invested, and then decides how much to invest accordingly. This setting naturally gives way to an investigation into subgame perfect Nash Equilibria (SPNE).

For this setting, we consider the proportional model, with the addition that, for simplicity and due to a small technicality addressed later, we assume that if no one invests, the last miner gets the reward with 0 investment.

There are several advantages to examining equilibria in this setting as opposed to the standard Nash Equilibria. This setting may be more realistic than Nash Equilibria, since in the real world miners will have the opportunity to invest in some time-based sequence, as opposed to them all choosing an amount and investing all at once, since some miners may learn about the opportunity later than others, and may be interested in investing a particular amount only when conditioned on the activity thus far. Another advantage is that in general, Nash Equilibria may not always exist. Consider the case with 1 miner for instance: if they invest 0, then they get no reward, but for any nonzero investment, they get reward 1 and are equally happy. There is no best response since their set of desirable responses has an open lower bound, and they way to invest a minimum on this interval.

Subgame Perfect Nash Equilibria, however, always exist, given certain conditions. We will prove that our setting does indeed give an SPNE, and hope to, in the future, continue by investigating the nature of centralization of equilibria in this setting, relative to the centralization of standard Nash Equilibria. While we have obtained partial results in this setting in simple cases, the results are not satisfactory for making concrete claims about centralization. We hope this to be a route of further possible research.

2.1 This Paper's Results

The first several results relate to the generalized multiplicative factors as described above, thus we let

$$x_i(q) = \frac{q_i^\alpha}{\sum_j q_j^\alpha} f(q)$$

where $f \in \mathcal{F}$ as defined above. We will call this an f-factor EoS reward model.

Theorem 2.1: *Let q be an equilibrium in an f-Factor EoS reward model and let $q_i \geq q_j > 0$, then $c_i \leq c_j$ and $c_i = c_j \iff q_i = q_j$.*
We see that this gives a direct parallel for Weinberg's result listed as Corollary 1.2.2. This result is used primarily as a tool for proving other results, but also gives the insight that having lower costs implies at least as much investment in equilibrium as those with higher costs.

Theorem 2.2: *For all pairs of miners i and j that participate in an equilibrium q in an f-factor EoS reward model, we have:*

$$\frac{x_i(q)}{f(q)} \geq 1 + \frac{1}{\alpha}\frac{q_i}{f(q)}\frac{\partial}{\partial q_i} f(q) - \frac{c_i}{c_j}\frac{1}{\alpha}$$

This gives a parallel for Weinberg's result listed as Theorem 1.2., that reduces to it in the case where $f(q) = 1$. We see that the rewards are naturally rescaled via division by $f(q)$ so that the left quantity of the inequality sums to 1 across all miners. We also see that since the right side matches Weinberg's result except with an additive factor, this bound gives a stronger guarantee of centralization. Before, we could obtain bounds on the number of miners that participate as a function of the differing costs and α, where the constraint came from the rewards having to add to 1. Here we see that, with an additional additive factor, they can only add

to 1 more quickly. Furthermore, given that a minor invests, this gives a weakly-greater lower-bound on their investment. Note that we have the stronger centralization guarantee, since for nonzero additive terms, each miner who invests in the equilibrium much invest a larger proportion than they did without the f-factor reward, but it's impossible for every miner's proportion to increase. This implies that, given that the bound is tight, in the worst case, some miner who invested before would not invest in the equilibrium with f-factor reward.

Lemma 2.2.1: *For miner i with nonzero investment in an equilibrium q in an f-factor EoS reward model:*

$$\frac{x_i(q)}{f(q)} \geq 1 + \frac{1}{\alpha}\frac{q_i}{f(q)}\frac{\partial}{\partial q_i}f(q) - \frac{1}{\alpha}. \tag{1}$$

Parallel to Weinberg's result listed as Corollary 1.2.1, and giving a correspondingly lower maximum number of participating miners, depending on f.

Theorem 2.3: *Assume there are countably infinitely many miners, and let $T = \sum_i q_i$, then there exists a Nash Equilibrium if and only if either:*

(1) *There exists a unique equilibrium in which only finitely many miners participate, as in Theorem 1.1, or:*

(2) *There exists a unique equilibrium in which countably infinitely many miners participate, in which case the investing miners' costs must be able to be listed in increasing order. All miners who have costs between 0 and the first limit point l of the costs participate, and for such an equilibrium to exist, we must have exactly $\lim_{n\to\infty}\sum_{i=1}^{n}(c_i - 1/T) = \lim_{n\to\infty} c_n = 1/T$.*

Theorem 2.4: *Consider n miners with costs $c_1, ..., c_n$ such that each miner chooses to invest some amount q_i in sequence according to their indices. Assume each miner gets payoff at the end of the game according to the proportional model, and that if no one invests, then the miner with greatest index gets reward 1 with no investment. In this setting, there exists a subgame perfect Nash equilibrium.*

Theorem 2.5: *In the 2-miner case, when the lower-cost miner goes first and given that both miners invest, the two miners' investment proportions differ by weakly more than in the standard Nash equilibrium, with equality only when there is equal cost.*
This fits our informal definition of being more centralized. When considering centralization to be variance, it also corresponds to more centralization, since the disparity in ownership of the reward becomes greater. Intuitively, it seems to be the case that going in order, given that you have the better cost, can't make you get lower reward; the only difference is that you have the opportunity to commit, and thus possibly block/scare out the other investors by claiming a larger portion of investment.

3 Equilibria for f-Factor Rewards

Let

$$x_i(q) = \frac{q_i^\alpha}{\sum_j q_j^\alpha} f(q)$$

where $f \in \mathcal{F}$ as defined above.

Theorem 2.1: *Let q be an equilibrium in an f-Factor EoS reward model and let $q_i \geq q_j > 0$, then $c_i \leq c_j$ and $c_i = c_j \iff q_i = q_j$.*

Proof of Theorem 2.1: We begin by noting that

$$\begin{aligned}\frac{\partial}{\partial q_i}x_i(q) &= \frac{\alpha q_i^{\alpha-1}}{\sum_j q_j^\alpha}f(q) - \frac{\alpha q_i^{2\alpha-1}}{(\sum_j q_j^\alpha)^2}f(q) + \frac{q^\alpha}{\sum_j q_j^\alpha}\frac{\partial}{\partial q_i}f(q) \\ &= \frac{\alpha x_i(q)}{q_i}(1 - \frac{x_i(q)}{f(q)} + \frac{1}{\alpha}\frac{q_i}{f(q)}\frac{\partial}{\partial q_i}f(q))\end{aligned} \tag{2}$$

Thus, since we know that we are looking for the scenario where i's utility is maximized, we consider $\frac{\partial}{\partial q_i}U_i(q) = \frac{\partial}{\partial q_i}x_i(q) - c_i$ if they spend something nonzero (as we assumed - otherwise $q_i = 0$), and see that:

$$c_i q_i = \alpha x_i(q)(1 + \frac{1}{\alpha}\frac{q_i}{f(q)}\frac{\partial}{\partial q_i}f(q) - \frac{x_i(q)}{f(q)}) \tag{3}$$

Before proceeding, we prove a lemma.

Lemma 2.2.1: *For miner i with nonzero investment in an equilibrium q in an f-factor EoS reward model:*

$$\frac{x_i(q)}{f(q)} \geq 1 + \frac{1}{\alpha}\frac{q_i}{f(q)}\frac{\partial}{\partial q_i}f(q) - \frac{1}{\alpha}. \tag{4}$$

Proof of Lemma 2.2.1: We note that, given that miner i participates in equilibrium, they get non-negative utility from doing so, thus from (2) we have:

$$\begin{aligned}&x_i(q) \geq c_i q_i \geq \alpha x_i(q)(1 + \frac{1}{\alpha}\frac{q_i}{f(q)}\frac{\partial}{\partial q_i}f(q) - \frac{x_i(q)}{f(q)}) \\ &\implies \frac{1}{\alpha} \geq 1 + \frac{1}{\alpha}\frac{q_i}{f(q)}\frac{\partial}{\partial q_i}f(q) - \frac{x_i(q)}{f(q)} \\ &\iff \frac{x_i(q)}{f(q)} \geq 1 + \frac{1}{\alpha}\frac{q_i}{f(q)}\frac{\partial}{\partial q_i}f(q) - \frac{1}{\alpha}.\end{aligned} \tag{5}$$

Note that here we needed the assumption that $x_i(q) \neq 0$, and thus there was nonzero investment by miner i, so that we can divide to transition between the first two equations above.

Proof of Theorem 2.1 cont.: Now we note that $\exists \epsilon > 0$ such that $x_i(q) = (1+\epsilon)x_j(q) \implies q_i = (1+\epsilon)^{1/\alpha}q_j$.

$$\begin{aligned}\implies c_i q_i &= \alpha(1+\epsilon)x_j(q)(1 + \frac{1}{\alpha}\frac{q_j}{f(q)}\frac{\partial}{\partial q_j}f(q) - (1+\epsilon)\frac{x_j(q)}{f(q)}) \\ &= (1+\epsilon)\alpha x_j(q)(1 + \frac{1}{\alpha}\frac{q_j}{f(q)}\frac{\partial}{\partial q_j}f(q) - \frac{x_j(q)}{f(q)}) - \epsilon(1+\epsilon)\frac{\alpha x_j(q)(1 + \frac{1}{\alpha}\frac{q_j}{f(q)}\frac{\partial}{\partial q_j}f(q) - \frac{x_j(q)}{f(q)})\frac{x_j(q)}{f(q)}}{(1 + \frac{1}{\alpha}\frac{q_j}{f(q)}\frac{\partial}{\partial q_j}f(q) - \frac{x_j(q)}{f(q)})} \\ &= (1+\epsilon)c_j q_j(1 - \epsilon\frac{\frac{x_j}{f(q)}}{1 + \frac{1}{\alpha}\frac{q_j}{f(q)}\frac{\partial}{\partial q_j}f(q) - \frac{x_j(q)}{f(q)}}) \\ \implies c_i(1+\epsilon)^{1/\alpha}q_j &= (1+\epsilon)c_j q_j(1 - \epsilon\frac{\frac{x_j}{f(q)}}{1 + \frac{1}{\alpha}\frac{q_j}{f(q)}\frac{\partial}{\partial q_j}f(q) - \frac{x_j(q)}{f(q)}}) \\ \implies c_i/c_j &= (1+\epsilon)^{1-1/\alpha}(1 - \epsilon\frac{\frac{x_j}{f(q)}}{1 + \frac{1}{\alpha}\frac{q_j}{f(q)}\frac{\partial}{\partial q_j}f(q) - \frac{x_j(q)}{f(q)}})\end{aligned} \tag{6}$$

We note that when $\epsilon = 0$, we have that the right hand side is 1, thus it remains to show that the derivative with respect to ϵ of it is negative on $(0, \infty)$, in which case $c_i < c_j$ as desired.
From Lemma 1, dividing (3) by (4), we get

$$\frac{\frac{x_j(q)}{f(q)}}{1 + \frac{1}{\alpha}\frac{q_j}{f(q)}\frac{\partial}{\partial q_j}f(q) - \frac{x_j(q)}{f(q)}} \geq \alpha + \frac{q_j}{f(q)}\frac{\partial}{\partial q_j}f(q) - 1$$

$$\implies c_i/c_j \leq (1+\epsilon)^{1-1/\alpha}(1 - \epsilon(\alpha + \frac{q_j}{f(q)}\frac{\partial}{\partial q_j}f(q) - 1)).$$

Now we let $h(\epsilon) = (1+\epsilon)^{1-1/\alpha}(1 - \epsilon(\alpha + \frac{q_j}{f(q)}\frac{\partial}{\partial q_j}f(q) - 1))$, then:

$$\begin{aligned} h'(\epsilon) &= (1+\epsilon)^{-1/\alpha}(1-1/\alpha)(1 - \epsilon(\alpha + \frac{q_j}{f(q)}\frac{\partial}{\partial q_j}f(q) - 1)) - (1+\epsilon)^{1-1/\alpha}(\alpha + \frac{q_j}{f(q)}\frac{\partial}{\partial q_j}f(q) - 1) \\ &= (1+\epsilon)^{-1/\alpha}(\frac{\alpha - 1}{\alpha} - \epsilon\frac{(\alpha-1)(\alpha + \frac{q_j}{f(q)}\frac{\partial}{\partial q_j}f(q) - 1)}{\alpha} - (\alpha + \frac{q_j}{f(q)}\frac{\partial}{\partial q_j}f(q) - 1)(1+\epsilon)) \end{aligned} \tag{7}$$

Since $f(q)$ is positive and weakly monotone increasing, its derivative is positive as well; we have:

$$\leq (1+\epsilon)^{-1/\alpha}(\frac{\alpha-1}{\alpha} - \epsilon\frac{(\alpha-1)^2}{\alpha} - (\alpha-1)(1+\epsilon)) \leq (1+\epsilon)^{-1/\alpha}(\frac{\alpha-1}{\alpha} - (\alpha-1)) \leq 0$$

Where the last inequality is since $\epsilon \geq 0$ and $\alpha \geq 1$. This concludes the proof of Theorem 2.1.

As a final note here, we see that we don't technically need $f(q)$ to be weakly monotone increasing in order to get the desired result, instead we need only that $h'(\epsilon) \leq 0$, and thus any f giving this condition would be sufficient.

Theorem 2.2: *For all pairs of miners i and j that participate in an equilibrium q in an f-factor EoS reward model, we have:*

$$\frac{x_i(q)}{f(q)} \geq 1 + \frac{1}{\alpha}\frac{q_i}{f(q)}\frac{\partial}{\partial q_i}f(q) - \frac{c_i}{c_j}\frac{1}{\alpha}$$

Proof of Theorem 2.2: Assume without loss of generality that $c_i \leq c_j$, otherwise the result is immediate from Lemma 2.2.1. Then by Theorem 1, $q_j \leq q_i$, and dividing two instances of (2), we have:

$$\begin{aligned} \frac{c_i}{c_j}\frac{q_i}{q_j} &= \frac{x_i(q)(1 + \frac{1}{\alpha}\frac{q_i}{f(q)}\frac{\partial}{\partial q_i}f(q) - \frac{x_i(q)}{f(q)})}{x_j(q)(1 + \frac{1}{\alpha}\frac{q_j}{f(q)}\frac{\partial}{\partial q_j}f(q) - \frac{x_j(q)}{f(q)})} \\ \implies 1 + \frac{1}{\alpha}\frac{q_i}{f(q)}\frac{\partial}{\partial q_i}f(q) - \frac{x_i(q)}{f(q)} &= \frac{c_i}{c_j}(\frac{q_j}{q_i})^{\alpha-1}(x_j(q)(1 + \frac{1}{\alpha}\frac{q_j}{f(q)}\frac{\partial}{\partial q_j}f(q) - \frac{x_j(q)}{f(q)})) \\ &\leq \frac{c_i}{c_j}\frac{1}{\alpha} \\ \implies x_i(q) &\geq f(q)(1 + \frac{1}{\alpha}\frac{q_i}{f(q)}\frac{\partial}{\partial q_i}f(q) - \frac{c_i}{c_j}\frac{1}{\alpha}) \\ \implies \frac{x_i(q)}{f(q)} &\geq 1 + \frac{1}{\alpha}\frac{q_i}{f(q)}\frac{\partial}{\partial q_i}f(q) - \frac{c_i}{c_j}\frac{1}{\alpha} \end{aligned} \tag{8}$$

Where we substituted using equation (4) to get the first inequality, and then used that $q_j/q_i \leq 1$.

Example: Conclusions for the Popularity Factor Model

We see that these results give immediate conclusions for the popularity factor model. Recall that we have, for $0 \leq \beta < 1$:

$$y_i(q) = \frac{q_i^\alpha (\sum_j q_j)^\beta}{\sum_j q_j^\alpha}$$

Thus here, $f(q) = (\sum_j q_j)^\beta$, which is positive since investments are non-negative, symmetric with respect to the miners, and which has partial derivatives

$$\frac{\partial}{\partial q_i} f(q) = \beta (\sum_j q_j)^{\beta - 1} \geq 0$$

since $\beta \geq 0$ and $q_j \geq 0$ for all j. Thus $f \in \mathcal{F}$ as desired, and the conclusions shown thus far apply. Most importantly, from Theorem 2.2, we have that, for miners i, j with nonzero investment:

$$\begin{aligned} & \frac{q_i^\alpha}{\sum_j q_j^\alpha} \geq 1 + \frac{\beta}{\alpha} \frac{q_i}{(\sum_j q_j)^\beta} (\sum_j q_j)^{\beta - 1} - \frac{c_i}{c_j} \frac{1}{\alpha} \\ \implies & \frac{q_i^\alpha}{\sum_j q_j^\alpha} \geq 1 + \frac{\beta}{\alpha} \frac{q_i}{\sum_j q_j} - \frac{c_i}{c_j} \frac{1}{\alpha} \end{aligned} \tag{9}$$

Thus confirming that, if one's reward corresponds to more utility the more total investment there is from the miners, then those who do invest are guaranteed a larger proportion of the total reward than in just the EoS model. Indeed, for β nonzero, this gives a strictly higher lower bound on the α-scaled proportion of investment. Since not all of the investors can increase their proportion of investment, this also gives a bound of strictly fewer miners investing in the case where $\beta \neq 0$, than for the original EoS setting.

4 Equilibria with Countably Infinitely Many Miners

We now consider the proportional model with countably infinitely many miners.

Theorem 2.3: *Assume there are countably infinitely many miners, and let $T = \sum_i q_i$, then there exists a Nash Equilibrium if and only if either:*

(1) *There exists a unique equilibrium in which only finitely many miners participate, as in Theorem 1.1, or:*

(2) *There exists a unique equilibrium in which countably infinitely many miners participate, in which case the investing miners' costs must be able to be listed in increasing order. All miners who have costs between 0 and the first limit point l of the costs participate, and for such an equilibrium to exist, we must have exactly $\lim_{n\to\infty} \sum_{i=1}^n (c_i - 1/T) = \lim_{n\to\infty} c_n = 1/T$.*

Proof of Theorem 2.3: We first note that Weinberg's results for the Nash Equilibra in which only finitely many miners participate, as in Theorem 1.1, still holds here, so long as there still exists an $i^* = \max\{i | c_i < T_i\}$, this gives condition (1) in Theorem 2.3. However, with countably infinitely many miners, it may sometimes be the case that no such maximum exists. We investigate these cases below.

Lemma 2.3.1: *In the above setting, if infinitely many miners participate in an equilibrium of the proportional model, their costs must have a limit point.*

Proof of Lemma 2.3.1: We first note that their costs must be bounded below by 0. If their costs were not bounded above, then we must have miners of arbitrarily high cost relative to one another participating,

but Theorem 2.2, with $f(q) = 1$ and $\alpha = 1$ gives Weinberg's Corollary 1.1.2 - that if miner i participates in equilibrium, than for all j, $x_j(q) \geq 1 - \frac{c_j}{c_i}$ - without reliance on only finitely many miners participating, and thus tells us that no two miners can participate in equilibrium with costs off by a factor of more than 100%. Thus we see that their costs are bounded, and all lie on $\mathbb{R}$, thus by the Bolzano-Weierstrass theorem, they must contain a limit point, call it l.

Lemma 2.3.2: *In the described setting, l acts as an upper bound on the participating miner's costs, and all miners in the interval [0,l) participate.*

Proof of Lemma 2.3.2: We assume that there exists a setting in which there is a limit point of the costs of participating miners, but that this limit point is not an upper bound on their costs. Let some participating miner thus have cost $c_k > l$, then for any $0 < \epsilon < c_k - l$, there are infinitely many miners with costs in the interval $(l - \epsilon, l + \epsilon)$. We know by the proof of Lemma 2.3.1 that, as per Corollary 1.1.2, if miner i has costs $x\%$ lower than miner j, then miner i must invest at least $x\%$ of the total investment in equilibrium.

We fix an $0 < \epsilon < c_k - l$, then as stated, there are infinitely many miners with costs in $(l - \epsilon, l + \epsilon)$, but as these costs are all bounded away from c_k, each of these infinitely many miners has some percentage of cost lower than miner k, bounded away from 0, call it δ. Thus each of the infinitely many miners must have at least $\delta\%$ of the total investment in equilibrium, which by the Archimedian property of $\mathbb{R}$, implies that the total investment exceeds 100% of itself, a contradiction.

Finally we note that all miners in the interval $[0, l)$ participate by Theorem 2.1, with $f(q) = 1$ and $\alpha = 1$, since for all potential miners i with costs in the interval, there must exist a participating miner j with cost above them (as they can get arbitrarily close to l), and thus $c_i \leq c_j \implies q_j \leq q_i$ so miner i must participate as well. Miners with cost l do not participate, as will be shown below.

Lemma 2.3.3: *For $T = \sum_i q_i$, $T < \infty$.*

Proof of Lemma 2.3.3: Recall that $U_i(q) = x_i(q) - c_i q_i \geq 0$ for each miner participating in equilibrium. Thus we have:

$$\begin{aligned} &\sum_i U_i(q) = 1 - \sum_i c_i q_i \geq 0 \\ &\implies 1 \geq \sum_i c_i q_i \geq \sum_i c_1 q_i = c_1 T \\ &\implies T \leq 1/c_1 < \infty \end{aligned} \tag{10}$$

Proof of Theorem 2.3 cont.: Now we note that, for an equilibrium to exist, there must exist a strategy profile of actions for the miners such that each miner is best responding - that is to say, each is getting optimal utility, given the strategy profile of the other miners. Thus we consider some potential equilibrium q, in which miner i invests q_i possibly 0. We give the condition for them to be best responding as follows. Consider some alternate potential investment q_i' and corresponding q'. Then $U_i(q') = \frac{q_i'}{T - q_i + q_i'}$ and so we have:

$$\frac{\partial}{\partial q_i'} U_i(q') = \frac{1}{T - q_i + q_i'} - \frac{q_i'}{(T - q_i - q_i')^2} - c_i = \frac{T - q_i - c_i(T - q_i - q_i')^2}{(T - q_i + q_i')^2}$$

Setting this equal to 0 and solving gives miner i's best response to be $\max\{0, \sqrt{(T - q_i)/c_i} - (T - q_i)\}$.

Thus for i participating in the equilibrium, we have

$$\begin{aligned} q_i &= \sqrt{(T-q_i)/c_i} - (T-q_i) \\ \implies q_i &= T - c_i T^2 \\ \implies \sum_{i\in S} q_i = T &= \sum_i (T - c_i T^2) \\ \implies 1/T &= \sum_i (1/T - c_i) \end{aligned} \tag{11}$$

and we see that in order for the above sum to converge, which it must in equilibrium since $1/T$ is a constant, $\lim_i c_i = 1/T$ and thus we must have that $T = 1/l$ where l is the first limit point.

From the above lemmas, if there is an equilibrium in which infinitely many miners participate, we now almost know exactly which miners will participate: those with costs between 0, and the first limit point. We verify that miners with cost at the limit point do not participate in the equilibrium.

$$\begin{aligned} \lim_{n\to\infty} \sum_{i\le n} (\sqrt{(T-q_i)/c_i} - T + q_i) &= T \\ \lim_{n\to\infty} \sum_{i\le n} \sqrt{(T-q_i)/c_i} &= \lim_{n\to\infty} nT \\ \lim_{n\to\infty} \frac{\sum_{i\le n} \sqrt{(T-q_i)/c_i}}{n} &= T \\ \implies \lim_{i\to\infty} \sqrt{(1/l - q_i)/l} &= 1/l \end{aligned} \tag{12}$$

which, if $q_i > 0$, gives that $\lim_{i\to\infty} q_i \to 0$, and so its limit point can't be nonzero, or it would contradict Theorem 2.1.

To conclude the proof of Theorem 2.3, we note that finding a T satisfying the above conditions is sufficient for showing an equilibrium exists. Note that if such a T exists, then we will have that $q_i = T - c_i T^2$ for each miner i in the participating interval, and these investments represent best responses for these miners by construction, since by the assumption that no finite equilibrium exists due to no maximal i^*, these investments must give nonnegative utility, and thus $\max\{0, \sqrt{(T-q_i)/c_i} - (T-q_i)\} \neq 0$ and they all invest the described amount.

5 Subgame Perfect Nash Equilibria in the Proportional Model

Proof of Theorem 2.4: *Consider n miners with costs $c_1, ..., c_n$ such that each miner chooses to invest some amount q_i in sequence according to their indices. Assume each miner gets payoff at the end of the game according to the proportional model, and that if no one invests, then the miner with greatest index gets reward 1 with no investment. In this setting, there exists a subgame perfect Nash equilibrium.*

First we will prove that the investment of miner i in equilibrium (if one exists), is continuous in the investments of each other miner. Let Q be the total investment of all miners besides i, then:

$$U_i(q) = \frac{q_i}{Q + q_i} - c_i q_i$$

so setting the derivative equal to zero, and solving for q_i gives

$$q_i = \sqrt{\frac{Q}{c_i}} - Q$$

which is continuous in Q as desired.

Now we note that the investment of each miner i is bounded above by $1/c_i$, since they can't get reward greater than 1, and this investment gives total cost 1, investing more will always give negative utility, in which case they prefer not to invest at all. (This also implies that the value we computed above must be a maximum, instead of a minimum.)

We now prove the theorem via backwards induction on n, the number of miners.

As our base case, we first note that if miners $2, ..., n$ always have best responses, then since miner 1s utility function is continuous in the other investments and its own, and since the investments are all bounded, we have a continuous function on a compact set, and thus by the extreme value theorem, it achieves its maximum, and thus miner 1 has a best response.

For each remaining miner, we have the same situation, except that some of the investments are now fixed, thus each miner has a best response.

Finally we note that we give the reward to the last miner if no one invests so that there is always reward 1 given. This ensures that the utility functions of the miners are continuous. Otherwise, we have the corner case that gave no equilibria in the single-miner case, where the utility function is not continuous in investment, since a miner may get reward 1 for an investment on an open interval, but 0 otherwise.

Thus we've proven that, in the given setting, a subgame perfect Nash equilibrium must always exist. We see as simple corollaries from the proof that this equilibrium consists of pure strategies and is the unique equilibrium in this setting, as is standard for such equilibria.

Proof of Theorem 2.5: *In the 2-miner case, when the lower-cost miner goes first and given that both miners invest, the two miners' investment proportions differ by weakly more than in the standard Nash equilibrium, with equality only when there is equal cost.* We first note that in the original Nash equilibrium setting, the investment proportions (by Theorem 1.1) are $c_2/(c_1 + c_2)$ and $c_1/(c_1 + c_2)$, for miners 1 and 2 respectively. We now consider the new setting. By the algebra in the proof of theorem 2.4, but replacing q_i and Q with q_1 and q_2, we obtain a system of two equations, which can be

References

[1] Coindesk. Bitcoin price index - real-time bitcoin price charts.

[2] Hashrate distribution, 2017.

[3] S. Matthew Weinberg. Bitcoin: A natural oligopoly. 2018.